70. The method of claim 69, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.

71. The method of claim 70, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.

72. The method of claim 69, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.

73. The method of claim 72, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.

74. The method of claim 69, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.

75. The method of claim 69, wherein integrating further comprises invoking countermeasures to a suspected attack.

76. The method of claim 69, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.

5 1
~~77~~. The method of claim ~~69~~, wherein the enterprise network is a TCP/IP network.

6 1
~~78~~. The method of claim ~~69~~, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.

11 9
~~79~~. The method of claim ~~72~~, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.

12
~~80~~. An enterprise network monitoring system comprising:

BV

a plurality of network monitors deployed within an enterprise network, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};

said network monitors generating reports of said suspicious activity; and

one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

18 12
~~81~~. The system of claim ~~80~~, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.

19 18
82. The system of claim 81, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.

20 12
83. The system of claim 80, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.

21 20
84. The system of claim 83, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.

B2

13 12
85. The system of claim 80, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.

14 12
86. The system of claim 80, wherein the integration further comprises invoking countermeasures to a suspected attack.

15 12
87. The system of claim 80, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.

16 12
~~88~~. The system of claim ~~80~~, wherein the enterprise network is a TCP/IP network.

17 12
~~89~~. The system of claim ~~80~~, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.

B2 Cont.

22 20
~~90~~. The system of claim ~~83~~, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.

In the Abstract:

Please delete the abstract and add:

B3

--A computer-automated method of hierarchical event monitoring and analysis within an enterprise network including deploying network monitors in the enterprise network, detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}, generating, by the monitors, reports of the suspicious activity, and automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.--

B